

Digital assets, auditor IT experience, and material misstatements: Evidence from a developing

country

Osama Abouelela^{1,2}, DAhmed Diab^{3,4*}, DSafaa Saleh⁵

¹Accounting Department, Imam Muhammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia.
 ²Accounting Department, Faculty of Business, Alexandria University, Alexandria, Egypt.
 ³Accounting Department, Prince Sultan University, Riyadh, Saudi Arabia.
 ⁴Faculty of Commerce, Beni-Suef University, Beni-Suef, Egypt.
 ⁵Accounting Department, Faculty of Business, Alexandria University, Alexandria, Egypt.

Corresponding author: Ahmed Diab (Email: adiab@psu.edu.sa)

Abstract

Keeping up with the global debate around cryptocurrencies, our study examines the relationship between cryptocurrency recognition and assessing the risks of material misstatement (RMM) and the possible moderating effect of auditor IT expertise on this relationship. We conducted a 2x2 factorial experimental design involving 130 auditors employed by licensed accounting and auditing firms. The results suggest that the presence of cryptocurrency in financial statements significantly increases the assessed RMM, especially among auditors with higher IT expertise. Sensitivity analysis supports these results. These findings have important implications for audit practices, highlighting the need for advanced IT training and specialized expertise for auditors involved in cryptocurrency audits. In line with agency theory, this study demonstrates the role of IT expertise in mitigating information asymmetry related to complex and emerging technologies. Moreover, our findings have practical implications since regulators, standard setters, audit firms, and educators can benefit from the findings, which emphasize the critical role of auditor competence in cryptocurrency matters and the value of regulatory oversight in promoting sound audit practices in this emerging area. In addition, our study fills a knowledge gap by providing recent evidence from a developing country.

Keywords: Auditor IT expertise, Cryptocurrency, Digital assets, Egypt, Material misstatement risks.

Funding: This study received no specific financial support.

History: Received: 31 January 2025 / Revised: 5 March 2025 / Accepted: 11 March 2025 / Published: 14 March 2025

Copyright: © 2025 by the authors. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

Competing Interests: The authors declare that they have no competing interests.

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Acknowledgment: The authors would like to thank Prince Sultan University for their support.

Publisher: Innovative Research Publishing

DOI: 10.53894/ijirss.v8i2.5402

1. Introduction

The current business environment has witnessed a major transformation in processing transactions due to digitalization, which has changed standard practices and patterns. The value of a business is no longer primarily based on tangible assets like machinery or physical infrastructure in this digitally driven environment [1-4]. Digital assets play a crucial role in digital transformation, differing fundamentally from physical assets through their online accessibility and use across various devices, including computers, smartphones, smartwatches, and smart TVs [5, 6].

The increasing prevalence of companies like PayPal, Uber, and Facebook highlights a shift towards digital assets as a key driver of success. Rather than having a large physical presence, many prosperous businesses use digital assets to conduct business internationally. Despite not owning the cars it uses for transportation, Uber, for instance, operates in many countries through a digital application, which is its main asset value. Even though these digitally oriented businesses have few physical assets, they generate significant revenue from their digital assets and frequently outperform more established businesses with large physical assets [7, 8].

Given the increased complexity of using digital assets, auditors must implement the proper audit procedures to identify and assess the risk of material misstatements (RMM), which is the possibility that financial statements would contain fake or misleading information that could influence users' decisions, according to the International Standard on Auditing (ISA 315). Inherent risk and control risk are the two components of this risk. The potential for a particular account balance or transaction type to be misrepresented, either on its own or in combination with other misstatements, in the absence of internal controls, is known as inherent risk (IR). On the other hand, the risk that current internal controls will not be able to identify or prevent substantial misstatements is known as control risk (CR) [9].

Unlike physical goods, which require shipping, digital assets are delivered almost instantaneously via uploads and downloads upon purchase. Consequently, these intangible assets encompass diverse forms such as cryptocurrencies, PDF documents, video and presentation files (e.g., Word, PowerPoint), audio, and image files [5]. While cryptocurrency is a prominent example of a digital asset, serving as an electronically stored and transferred medium of exchange, the broader category of digital currencies encompasses various forms [10]. This includes not only virtual currencies and cryptocurrencies but also widely used products like gift cards, debit cards, airline rewards points, and credit card cash-back rewards. These diverse mediums share the common characteristic of possessing real-world value and facilitating the purchase of goods and services [11-13].

Cryptocurrency transactions, including buying, selling, and exchanges, are conducted entirely online and recorded chronologically in a digital ledger known as the Blockchain [14]. This technology organizes records into blocks, fostering trust and reducing transaction costs. From a professional accounting perspective, the recognition of digital assets necessita tes the verification of management assertions during financial statement audits [15]. Accordingly, assessing risks is a dynamic process that relies on the auditor's knowledge of the audit client's operations and internal control system, among others [16]. This raises more questions regarding the auditor's role in assessing the RMM when planning for an audit of a client who is involved in cryptocurrency transactions.

The volatile and complex nature of cryptocurrencies, compounded by the lack of a robust regulatory framework, contributes to a heightened RMM in financial statements [17, 18]. Research indicates that this risk, impacting both IR and CR, is further influenced by how audit clients recognize these digital assets. Therefore, companies, auditors, and accountants must exercise vigilance and implement necessary safeguards to maintain the accuracy of financial statements that include cryptocurrencies.

In this regard, expertise in information technology (IT) is a must. The expertise of an IT auditor is characterized by advanced knowledge, skills, and specialized experience in IT auditing, which allows them to navigate complex challenges and contribute significant value to the organization [19]. However, research (e.g., [20, 21]) consistently indicates that IT auditor expertise significantly impacts the assessment of RMM. This expertise is instrumental in enabling auditors to understand intricate systems, apply relevant auditing standards, conduct effective risk assessments, and communicate clearly with stakeholders, ultimately contributing to a reduced RMM and higher audit quality.

Concerning our study context, there are several motivations for conducting it in Egypt. First, it provides recent evidence from a developing country, filling a knowledge gap in the existing literature. Second, it enables comparisons with studies in other countries to enhance understanding of the level of RMM factors across diverse contexts. Third, it addresses the specific challenges and considerations related to cryptocurrency and auditing practices within the Egyptian professional practice setting. Lastly, there is a relative scarcity of experimental research in this novel area.

Accordingly, our study addresses the research gap in understanding the interplay between cryptocurrency, IT auditor expertise, and the assessment of RMM, particularly within the context of a developing country like Egypt. Specifically, our study aims to answer the following research questions: 1) Does the presence of cryptocurrency transactions in the financial statements influence auditors' assessment of RMM? 2) Does IT auditor expertise moderate the relationship between the presence of cryptocurrency transactions and auditors' assessment of RMM?

Therefore, the primary objective of our research is to investigate how the presence of cryptocurrency transactions in financial statements and IT auditor expertise interact to influence the RMM assessment. It first investigates the direct effect of cryptocurrency transactions on perceived misstatement risk, considering whether factors like valuation, accounting standards, and fraud susceptibility inherently increase risk. Second, it explores whether IT auditor expertise moderates this relationship, hypothesizing that higher expertise leads to greater sensitivity to cryptocurrency-related risks (e.g., blockchain, wallet security, decentralization), and conversely, that lower expertise may result in risk underestimation.

By conducting a field experiment involving 130 auditors employed by licensed accounting and auditing firms in Egypt and using the Wilcoxon Signed-Rank Test to analyze paired data, the results indicate a statistically significant increase in the

assessed RMM when cryptocurrency is present in financial statements. This suggests that auditors perceive a higher likelihood of material misstatements in the presence of cryptocurrency transactions compared to their absence. Furthermore, using the Mann-Whitney test, IT auditor expertise was found to significantly moderate this relationship, strengthening the positive association between cryptocurrency presence and assessed misstatementrisk. Sensitivity analysis corroborated these findings.

Our research holds both scientific and practical significance. Scientifically, it contributes to narrowing the expectations gap in auditing by enhancing auditors' ability to assess RMM. It also expands the body of knowledge on cryptocurrency auditing and audit quality by addressing a gap in previous research by focusing on the impact of IT auditor expertise on the relationship between a client's cryptocurrency holdings and the auditor's assessment of RMM. This contributes to the preparation of reliable financial statements. Practically, our research employs a field experiment to test its hypotheses, with the potential to improve auditors' professional judgment and risk assessment skills, thereby increasing public trust in the auditing profession and reducing litigation risk. The existing body of scholarly research addressing the interaction between cryptocurrencies and traditional financial markets within the Middle East and North Africa (MENA) region, particularly within Egypt, is relatively limited, which creates a significant opportunity for our study to contribute novel insights to the field and provide valuable guidance for policymakers and investors operating within this specific regional context.

The remainder of our study is structured as follows: Section Two presents the Egyptian context; Section Three provides a literature review and hypotheses development; Section Four details the research design; Section Five discusses the findings; and finally, Section Six summarizes and concludes the paper.

2. Egyptian Context

The selection of Egypt as the research setting is based on several key considerations. The Egyptian cryptocurrency market represents an emerging market exhibiting increasing levels of adoption and trading activity, thereby providing a pertinent context for investigating the impact of cryptocurrency volatility on established financial markets. Furthermore, the unique confluence of economic and regulatory factors within Egypt provides a distinct setting for examining the interplay between cryptocurrencies and stock market indices, potentially revealing dynamic relationships that diverge from those observed in developed economics with more mature and established regulatory frameworks. Finally, the focus on the Egyptian market allows for a nuanced examination of the impact of cryptocurrency volatility within an economic environment characterized by specific macroeconomic factors such as currency fluctuations, inflation rates, and distinct patterns of investor behavior, which may differ substantially from those observed in other market contexts [22, 23].

Regarding the Egyptian auditing context, the framework for assessing RMM is provided by the Egyptian Auditing Standard No. 315, issued by the Minister of Investment Decree No. 166 of 2008, which is aligned with the International Standards on Auditing (ISA) (Revised 2019), issued by the International Auditing and Assurance Standards Board (IAASB). Whether the misstatements are deliberate (fraud) or unintentionally made (error), this auditing standard specifies how auditors should recognize and evaluate the RMM in financial statements. Both the overall financial statements and the individual accounts, transactions, and disclosures are evaluated. Performing risk assessment procedures such as analytical procedures, inquiries, and observations; developing a thorough understanding of the entity and its surroundings; recognizing and evaluating risks at the assertion and financial statement levels; taking fraud risk into particular consideration; maintaining professional skepticism throughout the audit engagement; maintaining an objective and questioning mindset; remaining alert for any indicators that may be suggestive of material misstatements; and putting appropriate audit responses in place, including determining the nature, timing, and extent of such procedures; and carefully documenting all risk assessment procedures and findings are important auditor responsibilities [9, 24].

However, the regulatory framework governing cryptocurrencies in Egypt is established by the Central Bank and Banking Law No. 194 of 2020, which institutes stringent prohibitions on activities related to these digital assets. Article 206 of the aforementioned law explicitly prohibits the issuance, trading, promotion, creation, or operation of platforms facilitating th e trading of cryptocurrencies or electronic money, as well as the conduct of any ancillary activities related thereto, without explicit licensing granted by the Central Bank's Board of Directors under established rules and procedures. Article 225 of the same legislative act stipulates the penalties for contraventions of Article 206, which include potential imprisonment and/or substantial monetary fines ranging from one million to ten million Egyptian pounds.

Notwithstanding its regulatory stance on decentralized cryptocurrencies, the Central Bank of Egypt has declared its intention to create a Central Bank Digital Currency (CBDC), a project designed to establish a secure and efficient digital mechanism for payments and financial transfers. This initiative aims to provide customers with access to a digital representation of the Egyptian pound, directly linked to and backed by the Central Bank, facilitating seamless and expeditious daily transactions. As articulated within the Central Bank's Future Projects, this proposed CBDC constitutes an official, centrally issued digital currency, thereby differentiating it from decentralized, peer-to-peer cryptocurrencies such as Bitcoin.

There are several strategic reasons why the Central Bank of Egypt is looking at the possibility of issuing a digital currency as follows. Increasing financial inclusion by giving more people, especially those living in rural or underdeveloped areas and those not currently able to access traditional banking systems, access to formal financial services. The enhancement of payment system efficiency by lowering the expenses and processing times related to both domestic and international financial transactions. Additionally, using improved transaction traceability and monitoring capabilities to bolster safeguards against terrorist financing and other illegal financial activities, such as money laundering. Fostering the development of new digital financial services and the introduction of creative business models to promote innovation in the financial industry. Furthermore, the significant expenses related to the creation, handling, and distribution of physical currency should be

decreased. Finally, to be consistent with the changing global central banking environment, which is illustrated by the growin g acceptance and interest in CBDCs.

3. Literature Review and Hypotheses Development

3.1. Cryptocurrency: A background

Digital assets, crucial to understanding cryptocurrencies, are intangible resources existing as binary data, encompassing diverse forms from images and videos to online accounts [25-27]. These assets are defined by their value, usability, accessibility, and applicability [28], representing an organization's controlled and potentially economically beneficial electronic records [27]. Key characteristics include their intangible nature, reliance on digital systems, controllability, measurability, the potential for future economic benefits, unique digital identity, and tradability [29, 30]. Digital assets are categorized into cryptocurrencies (like Bitcoin), stablecoins (linked to stable assets), e-money tokens (for electronic payments), security tokens (representing fractional ownership), and utility tokens (granting access to products or services) [31].

The concept of cryptocurrency, a significant category of digital assets, centers on its function as a digital medium of exchange, operating independently of tangible currencies and lacking the backing of governmental or institutional entities [32]. Cryptocurrencies, exemplified by Bitcoin, are generated through software and complex mathematical algorithms, employing robust encryption protocols and blockchain technology to ensure transactional integrity and prevent unauthorized alteration Popescu [33]. Parampathu [34] defines cryptocurrency as a virtual, intangible digital currency produced by computer programs, operating outside the purview of central banking or official regulatory bodies, and employed for online commercial transactions and currency conversion, based on voluntary acceptance by users. Baur, et al. [35] further articulates cryptocurrency as a digital asset designed specifically to function as a medium of exchange, leveraging cryptography for decentralized control, secure transaction processing, management of unit creation, and verification of asset transfers.

Cryptocurrencies can be categorized based on their governance and management structures. Aysan, et al. [36] propose a taxonomy of community-driven coins, characterized by decentralization and susceptibility to market sentiment, and firmdriven coins, managed by corporate entities capable of market interventions. Similarly, Akyildirim, et al. [37] distinguish between firm-driven cryptocurrencies, managed by specific organizations for use within their operational environments (e.g., BNB, ADA, XRP), and community-driven cryptocurrencies, lacking corporate affiliation and governed by a distributed community on a decentralized infrastructure (e.g., BTC, ETH, DOGE).

As per Akyildirim, et al. [37] cryptocurrencies have several salient characteristics including (1) a pronounced price volatility, reflecting substantial and rapid fluctuations in market valuations; (2) a speculative investment profile, stemming from the lack of tangible asset backing and reliance on market dynamics for value determination; and (3) a high degree of susceptibility to investor sentiment, where news dissemination and media coverage exert a considerable influence on market behavior and price movements. However, there are also several potential costs associated with misstated cryptocurrency valuations, including financial losses for investors, reputational damage, regulatory penalties, increased audit fees, and the cost of implementing necessary internal controls [38].

Akyildirim, et al. [37] delineate several salient characteristics of cryptocurrencies. These include: (1) pronounced price volatility, reflecting substantial and rapid fluctuations in market valuations; (2) a speculative investment profile, stemming from the lack of tangible asset backing and reliance on market dynamics for value determination; and (3) a high degree of susceptibility to investor sentiment, with news dissemination and media coverage exerting a considerable influence on market behavior and price movements.

Synthesizing the preceding perspectives, we conclude that cryptocurrency can be defined as a virtual, intangible digital currency generated algorithmically, characterized by the absence of a predetermined lifespan, its independence from centralized regulatory bodies such as central banks, and its utilization as a digital medium of exchange facilitated by internet-based encryption and blockchain technology, which provides a distributed digital ledger for recording all transactions.

3.2. Accounting For and Auditing Cryptocurrencies

Given the absence of specific IFRS standards for cryptocurrencies, IAS 8 guides their accounting treatment, requiring management to develop relevant and reliable policies based on existing standards and the Conceptual Framework for Financial Reporting (IAS 8). It is argued that cryptocurrencies, due to their digital nature, should be treated as intangible assets under IAS 38, fulfilling the criteria of being non-monetary, identifiable, and lacking physical substance [39, 40]. These assets are not classified as cash, financial instruments, or inventory [40]. Cryptocurrency mining is considered the creation of an internally generated intangible asset recognized at a cost [40]. Subsequent measurement depends on the existence of an active market; those with active markets are measured at fair value, while others use the cost method. Cryptocurrencies with indefinite useful lives are not amortized but are subject to annual impairment testing (IAS 36; Procházka [41]). Under IAS 38, subsequent measurement can use either the cost or revaluation model; with the latter, revaluation surpluses are recognized in other comprehensive income until derecognition, while declines in fair value are recognized in profit or loss [42].

From the preceding examination, we conclude that cryptocurrencies, under their digital embodiment, constitute a subset of intangible assets and are thus governed by the provisions of IAS 38, Intangible Assets. This standard defines an intangible asset as a non-monetary asset that is identifiable and lacks physical substance. Consequently, recognition as an intangible asset under IAS 38 is contingent upon the fulfillment of the following criteria: (1) the asset must be non-monetary; (2) the asset must be both measurable and identifiable; and (3) the asset must lack physical existence.

Auditing cryptocurrencies requires professional judgment regarding materiality, considering both financial and non-financial factors [43]. A thorough risk assessment, evaluating inherent, control, and detection risks, is crucial [18, 44].

Inherent risk is generally high due to the novelty of these assets and the judgment involved in valuation, especially regarding impairment, often requiring consideration of IT risks. Control risk is also typically high due to difficulties in controlling fair value measurement, leading to an elevated RMM. Consequently, auditors must plan for low detection risk. Audit procedures include control tests (e.g., verifying transaction reviews and impairment testing) and substantive tests (analytical procedures and tests of details) to obtain sufficient appropriate audit evidence [18, 44].

Auditors' prior engagement with cryptocurrency assets can exert a significant in-fluence on their professional risk assessments. Auditors possessing prior experience with this asset class may exhibit a more nuanced understanding of the inherent risks involved, potentially leading to more accurate and informed risk evaluations. Further, entities with experience in cryptocurrency transactions may have implemented more robust internal control frameworks, which could mitigate certain categories of risk. The pre-vailing regulatory environment governing cryptocurrency transactions also plays a crucial moderating role. A well-defined and comprehensive set of accounting standards and regulatory guidelines can diminish ambiguity and enhance the consistency of risk assessments across the auditing profession [45].

RMM, as defined by ISA 315, is the risk of materially misstated financial statements before the audit, impacting users' economic decisions [46]. This risk can be viewed from the auditor's perspective (failure to detect misstatements) [47] or from the internal control perspective (failure to prevent, detect, or correct misstatements) [48]. A comprehensive definition includes the possibility of misstatements (from error or fraud), individually or aggregated, exceeding materiality, and influencing financial statement users. This risk comprises inherent risk (susceptibility of an account or transaction to misstatement without considering internal controls, e.g., cash transactions having higher inherent risk) [49] and control risk (risk of the internal control system failing to prevent, detect, or correct a material misstatement, e.g., insufficient cash disbursement controls) [50].

RMMs can manifest in several ways, including revenue recognition manipulation, manipulation of reserves, manipulation of capitalization and expenses, such as improperly capitalizing R&D expenditures, manipulation of disclosures, accounting estimates, and violations of accounting standards, such as GAAP or IFRS [51]. Therefore, RMM is a complex, multi-faceted process influenced by several contextual factors beyond IT expertise, including organizational culture, cryptocurrency experience, and regulatory environment. A risk-tolerant culture may accept cryptocurrencies, while a conservative culture may be more cautious. Open communication and professional skepticism within audit firms and client cultures can affect the thoroughness of risk assessments [52].

IT auditor expertise involves specialized knowledge and skills enabling effective evaluation of information systems, associated controls, and relevant risks to ensure data integrity in financial reporting [53]. This expertise encompasses several perspectives [54]: (1) Risk management, focusing on identifying, assessing, and mitigating IT-related risks like cybersecurity vulnerabilities and data breaches; (2) Technical knowledge, emphasizing proficiency in areas like information security, systems architecture, data analytics, and emerging technologies; (3) Professional standards compliance, highlighting adherence to relevant standards and guidelines (e.g., COBIT, ISO/IEC 27000); and (4) Audit quality, recognizing IT auditor expertise as crucial for high-quality audit outcomes in digitized environments, contributing to the reliability and integrity of the audit process.

3.3. Cryptocurrency Recognition and Assessing RMM

The expected association between cryptocurrency and assessing RMM is based on several theories [55, 56] perhaps the most important of which are the agency theory and the theory of money. Agency theory recognizes the potential for agency problems arising from the separation of ownership (shareholders) and control (management). Management (agents) may be incentivized to manipulate financial reporting, particularly concerning complex and opaque transactions such as those involving cryptocurrencies, to present a more favorable financial picture. This manipulation elevates RMM [56]. The theory of money delineates the core functions of money, such as a medium of exchange, a unit of account, a store of value, and a standard of deferred payment. Within the context of cryptocurrencies, this theory raises critical questions regarding the extent to which these digital assets effectively fulfill these functions and the consequent impact on risk assessment [55].

Empirical evidence from various studies (e.g., [17, 18, 31]) suggests a direct relationship between the recognition of cryptocurrencies in client financial statements and the assessment of RMM. These studies converge on the finding that client recognition of cryptocurrencies exerts a positive and statistically significant influence on auditors' assessments of inherent risk. Specifically, a greater degree of client recognition of cryptocurrency transactions corresponds to a higher level of inherent risk assigned by the auditor, which subsequently translates into an increased overall RMM.

In this regard, Smith and Srivastava [31] emphasize the importance of robust custody solutions for digital assets, highlighting risks, market stability, and investor confidence, and offering recommendations for managing digital assets with transparency and adherence to standards. Vincent and Wilkins [18] analyze audit challenges related to cryptocurrency recognition, focusing on the lack of regulatory guidance, increased inherent risk, technology and security risks, valuation complexities, and the need for enhanced training and audit tools. Harrast, et al. [17] empirically investigate the inherent risks of cryptocurrencies through a survey of audit and accounting professionals, demonstrating that cryptocurrency recognition significantly increases auditors' risk assessments, highlighting the need for robust methodologies and better training due to the lack of regulatory guidance. All three sources converge on the idea that recognizing digital assets, especially cryptocurrencies, in financial reports increases risk assessment for auditors and influences market dynamics.

The association between cryptocurrency transactions and the assessment of RMM is further compounded by several contextual factors within the Egyptian professional business environment, including the evolving regulatory landscape, the varying levels of auditor expertise in blockchain technology, and the general skepticism surrounding digital currencies.

Additionally, the lack of standardized guidelines for auditing cryptocurrency transactions can lead to increased uncertainty and heightened risks in financial reporting.

Considering the above discussion, the first hypothesis of this study can be derived as follows:

 $H_{1:}$ Cryptocurrency recognition positively affects the assessment of RMM.

3.4. The Moderating Effect of Auditor IT Expertise

The extant empirical research (e.g., [20, 57-59]) offers compelling evidence for a significant relationship between auditor IT expertise and the assessment of RMM. These studies report that variations in IT expertise among auditors result in discernible differences in their evaluations of these risks. Specifically, differences in IT expertise influence auditors' understanding of intricate technical systems, proficiency in the utilization of technical audit tools and techniques, comprehension of security risks and associated vulnerabilities, effectiveness in communicating and collaborating with IT professionals, and application of professionalskepticism within the context of IT-dependent business environments.

However, the studies cited in the previous paragraph have been criticized for disregarding the impact of auditor IT expertise on the association between cryptocurrency and assessing the RMM. We suggest that the interaction between auditor IT expertise and cryptocurrency can serve as a moderating variable, potentially influencing the direction and/or strength of the relationship between cryptocurrency and assessing RMM.

Specifically, auditors possessing higher levels of IT expertise are expected to demonstrate a greater capacity to comprehend the inherent complexities of cryptocurrency transactions, effectively identify associated risks—including those related to valuation, security, and regulatory compliance—and appropriately deploy relevant audit tools and techniques to evaluate the potential for material misstatement pertaining to cryptocurrency holdings and transactions. Conversely, audit ors with lower levels of IT expertise may experience significant impediments in accurately assessing these risks, potentially leading to incomplete or inaccurate risk assessments.

These challenges are further exacerbated by contextual factors specific to the Egyptian environment, including the evolving regulatory landscape governing crypto-currencies, the inherent market volatility of these digital assets, the absence of established accounting standards, and the fundamental complexity of blockchain technology [60]. Considering this discussion, the second hypothesis of this study can be de-rived as follows:

Based on previous studies that addressed the association between IT auditor expertise and the assessment of RMM, as well as the Egyptian context, the second hypothesis of this study can be derived as follows:

H₂: IT auditor expertise moderates the association between cryptocurrency recognition and the assessment of RMM.

4. Research Design

4.1. Sample selection

In a field experiment, participants are exposed to various treatments that are related to the manipulating independent variable, which is a common methodology in social science research. To put it another way, experiments can be utilized to assess people's opinions, desires, and cognitive capacities. Furthermore, by changing the independent variable and observing whether the change causes a change in the dependent variable in a controlled setting, experiments are suitable for estimating the relationships between variables and hypothesis-testing research that seeks to explore the proposed causation [61]. Accordingly, our experimental study aims to test the research hypotheses to conclude whether the Egyptian auditors' judgments regarding the assessment of RMM would be affected by the cryptocurrency transactions and whether this effect is modified by the experience of auditors in IT.

The study population involved both auditors and academics [62]. For primary analysis, it encompassed auditors employed within accounting and auditing firms, located in Cairo and Alexandria governorate, duly licensed to conduct audits of joint stock companies. A judgmental sample of 250 individual auditors was subsequently selected from this defined population, with the selection process guided by several key criteria designed to ensure a representative sample. These criteria included: (1) proportionate inclusion of auditors registered with the Egyptian Financial Supervisory Authority (EFSA) and those operating outside of EFSA registration; and (2) representation of both large and small accounting and auditing firms, encompassing both formally registered and unregistered entities [63].

For conducting additional analysis, a secondary study population was defined, consisting of academic personnel, specifically faculty members and assistant staff within the Accounting Departments of the Egyptian Faculties of Commerce at Alexandria and Damanhour Universities. A judgmental sample of 120 individual academics was subsequently drawn from this population. The sampling strategy prioritized the inclusion of individuals holding postgraduate qualifications, specific ally master's and doctoral degrees, with a particular emphasis on those specializing in the domains of auditing or financial accounting. Furthermore, efforts were undertaken to ensure a high degree of homogeneity within each stratum defined by academic qualification. Recognizing the inherent novelty and complexity of the subject matter under investigation, a supplementary experimental study was conducted with a student cohort to assess their level of awareness and comprehension of the research topic [63].

4.2. Variables' Measurement

4.2.1. Dependent Variable

For our study, the RMM assessment, the dependent variable, is operationally defined as the level of consensus achieved among the majority of study participants concerning the probability of misstatement occurring within a designated class of transactions or account balances. This assessment explicitly considers the potential for such misstatements to constitute a material misstatement, whether considered individually or when aggregated with other misstatements across various transaction classifications or account balances, under the explicit assumption of the absence of effective internal control policies, procedures, and related mechanisms. The assessed level of risk, which is conceptualized as a continuum ranging from high to low, incorporates both IR, defined as the susceptibility of an account balance or class of transactions to misstatement before the consideration of internal controls, and CR, defined as the risk that the entity's internal controls will fail to detect or prevent a material misstatement. The operationalization of this variable was achieved through the measurement of the degree of consensus among study participants regarding the appropriate professional judgment to be exercised in the assessment of RMM, where responses were elicited using an 11-point Likert scale ranging from 0%, representing a negligible level of associated risk, to 100%, representing a very high level of risk [17, 63].

4.2.2. Independent Variable

Cryptocurrency recognition serves as the independent variable for our study and is operationally defined as the inclusion or exclusion of digital cryptocurrencies recognized as intangibles on the balance sheet. The manipulation of this independent variable was achieved through the presentation of two distinct pilot case scenarios to the participating auditors. The first scenario consisted of financial statements that explicitly excluded any recognition of digital cryptocurrencies recognized as intangible assets, thereby creating a controlled comparison to assess the impact of cryptocurrency recognition on the dependent variable [63].

4.2.3. Moderating Variable

In our study, the auditor's IT expertise is operationalized as a moderating variable. This construct reflects the auditor's level of proficiency and practical experience across both the domains of accounting and auditing principles and the domain of information technology, specifically focusing on the technical aspects of IT systems, as this knowledge is most directly relevant to assessing risks associated with complex technical systems, such as those used in cryptocurrency transaction s. The IT domain encompasses familiarity with and practical application of various technologies, including accounting software applications, remote auditing methodologies, and the IT infrastructure and tools employed by the auditee. This moderating variable was operationalized as a binary variable, assigning a value of 1 to auditors demonstrating prior experience and expertise in information technology and a value of 0 to those lacking such demonstrable experience [58]. Figure 1 depicts the research model reflecting the relationships among research variables.



The research model.

4.3. The Experimental Study

4.3.1. Experimental Study Tools and Procedures

The questionnaire serves as the study instrument for data collection. Its design makes sense, and relevant statements are presented understandably. The purpose of the first portion is to gather data regarding the sample participants' demographics. Next, auditors participating in the experiment, who voluntarily took part in our study, were asked to consider that they were auditing a client's financial statements under two scenarios to investigate the influence of cryptocurrency recognition on the assessment of RMM. For academics, they were asked to assume the role of auditors. The first scenario presented participating auditors with a set of financial statements explicitly excluding any recognition of cryptocurrencies as intangible assets. The second scenario presented a parallel set of financial statements wherein cryptocurrencies were explicitly included as intangible assets. In both scenarios, participants were tasked with assessing the level of RMM specifically associated with the intangible asset balance. Data collection procedures involved multiple field visits to accounting and auditing firms during mid-June and July 2024, facilitating the direct hand delivery and subsequent retrieval of the experimental case materials, as well as providing participants with the opportunity to engage in discussions with the researcher and address any inquiries.

The experimental protocol involved the provision of a comprehensive information package to each participant. This package was designed to emulate a realistic audit engagement and contained the following components: (1) a descriptive profile of a hypothetical audit client, ABC Inc.; (2) a statement confirming the absence of any prior qualified audit opinions or restatements of financial statements by the audit client; (3) a summarized set of financial statements encompassing two fiscal periods, including a balance sheet, an income statement, a statement of cash flows, and pertinent accompanying notes; and (4) the two designed experimental case scenarios both with and without the inclusion of cryptocurrencies. Participants were asked to respond to the following experimental question: "Assume you plan to audit the financial statements of the attached case, please assess the level of RMM of the balance of intangible assets as of December 31, 2023, using an 11-point

Likert scale ranging from 0% (representing a negligible level of associated risk) to 100% (representing a very high level of risk), given that the hypothetical case has an effective internal control structure. This scale was designed to measure perceived risk of material misstatement, reflecting the auditor's judgment about the likelihood and potential magnitude of misstatements. Each 10-point increment on the scale represented a 10% increase in perceived risk" following some prior studies [62-64].

4.3.2. Experimental Design, Treatments, and Comparisons Experiment

The study employed a $2x^2$ factorial experimental design to rigorously test the formulated research hypotheses (Table 1). This design permitted the investigation of the main effects and potential interaction effects of two independent variables, each operationalized at two distinct levels. A third factor was maintained as a constant, effectively serving as a control condition or representing a variable not subject to experimental manipulation. Auditors were categorized into high and low IT expertise groups based on their responses to the IT expertise questions. Specifically, those scoring above the median on the composite IT expertise measure were classified as having high IT expertise, while those scoring at or below the median were classified as having low IT expertise. This median split approach is common practice in research involving the categorization of expertise. The specific questions used to assess IT expertise focused on the auditor's understanding of blockchain technology, cryptocurrency transactions, and related IT controls, aligning with the technical expertise definition provided earlier in this section.

Table 1. Experimental design, treatme	nts, and comparisons.			
Independent variable Moderating variable		Absence of cryptocurrencies among intangible assets	Presence of cryptocurrencies among intangible assets	
	high IT expertise (A)	(1)	(2)	
IT auditor expertise				
	low IT expertise (B)	(3)	(4)	

As indicated in Table 2, the experimental design consisted of four treatments, resulting from the combination of two factors: Cryptocurrency recognition (Present/Absent) and Auditor IT Expertise (High/Low). Treatment (1) involved auditors with high IT expertise auditing financial statements without cryptocurrencies. Treatment (2) involved auditors with high IT expertise auditing financial statements with cryptocurrencies. Treatment (3) involved auditors with low IT expertise auditing financial statements without cryptocurrencies. Finally, Treatment (4) involved auditors with low IT expertise auditing financial statements with cryptocurrencies. Under all treatments, participants were asked to assess the RMM.

By comparing participants' responses across treatments of the within-subjects Cryptocurrency recognition independent variable as a pre-test without recognition case versus a post-test with the recognition case, we can determine whether the presence of cryptocurrencies makes a difference in auditors' judgments, regardless of the effect of their IT experience, i.e., to test H1. However, to test for the IT auditor expertise moderating effect (H2), responses of the two independent groups (A and B) are compared to determine whether IT auditor expertise interacts with the presence of cryptocurrencies in affecting auditors' judgment about RMM.

It is crucial to recognize that experimental research is often susceptible to both external and internal sources of invalidity. We used the same statements to create a standardized questionnaire that addressed the instrumentation effect, adjusted for other potential influences on the dependent variable, and reversed the treatments' order within each group to counteract the order effect to improve internal validity. In addition, we conducted additional tests. To increase external validity, we conducted a field experiment in a more natural professional setting in addition to employing a sample of academics to assume the role of auditors as a sensitivity analysis.

5. Results and Discussion

5.1. Descriptive Statistics

For the primary analysis, a judgmental sample of 250 individual auditors employed within accounting and auditing firms licensed to conduct audits of joint-stock companies, including audit managers and senior auditors, was selected. For the sensitivity analysis, a judgmental sample of 120 individual academics consisting of the Egyptian Faculties of Commerce at Alexandria and Damanhour Universities was selected. Table 2 provides the distribution and retrieval of survey instruments, along with the calculated response rates, where the final sample for the primary analysis was 130 usable responses with a 52% response rate. For the other additional analysis, the final sample was 100 usable responses with an 83% response rate.

We acknowledge that the achieved response rate of 52% constitutes a limitation of the present research. A multi-faceted approach was adopted to maximize participant engagement and mitigate potential biases. This approach encompassed the development of a concise and user-friendly questionnaire, the utilization of multiple communication channels, the provision of a transparent explanation of the study's objectives and the significance of participant contributions, and the assurance of participant anonymity and data confidentiality. The timing of questionnaire distribution was also strategically considered to optimize response rates.

Table 2.

Sample group	Target population	Distributed	Usable responses	Response rate (%)
Auditors	Licensed Auditors of Joint Stock Companies	250	130	52
Academics	Accounting departments (Alexandria & Damanhour Universities)	120	100	83

The distributed and received experimental cases.

The reliability and internal consistency of the data collection instrument were evaluated using Cronbach's alpha. Cronbach's alpha is a widely utilized statistical measure of internal consistency reliability, assessing the degree to which multiple items within a scale measure the same underlying construct [63]. The coefficient generated by Cronbach's alpha ranges from 0 to 1, with values closer to 1 indicating greater internal consistency and therefore higher reliability. A conventional threshold for acceptable internal consistency is a coefficient exceeding 0.5. In the present study, the calculated Cronbach's alpha coefficient was 0.863, demonstrating a robust level of internal consistency and providing evidence that the data are suitable for subsequent statistical analysis and that the findings derived from the sample can be reasonably generalized to the larger study population.

Descriptive statistics for participants' responses on the Likert scale are presented in Table 3. Regarding the descriptive statistics for the sample of responses that addressed the first experimental case, in the absence of cryptocurrencies among the intangible assets, the minimum percentage of responses for assessing the RMM was 20%, while the maximum percentage was 65%, and the mean for those responses was 32.31%. In the second experimental case, under the presence of cryptocurrencies, the minimum percentage of responses for assessing the RMM was 50%, while the maximum percentage of responses was 83.85%. Additionally, 56% of respondents had experience in IT.

To make sure the participants understood the current experiment, we carried out a few preliminary checks. In general, the manipulation checks showed that the participants had a good understanding of the material that was given to them. More precisely, participants confirmed the existence of cryptocurrencies in the real presence of the experiment, indicating their broad comprehension of the information provided. Furthermore, if these items were indeed unavailable, every participant accurately identified their unavailability.

5.2. Main Findings

The determination of the appropriate statistical methodology for hypothesis testing necessitated an assessment of the distributional properties of the study variables. To this end, the Kolmogorov-Smirnov test, a widely recognized test for assessing normality, was employed [63]. The null hypothesis under consideration posited that the population from which the study sample was drawn conformed to a normal distribution, while the alternative hypothesis asserted a deviation from normality. The results of the Kolmogorov-Smirnov test yielded a p-value of 0.000 for all variables under investigation, which falls below the conventional significance threshold of $\alpha = 0.05$. This outcome led to the rejection of the null hypothesis of normality in favor of the alternative hypothesis, thereby establishing the non-normality of the data. As a consequence of this finding, non-parametric statistical procedures were deemed appropriate and were subsequently utilized for the formal testing of the research hypotheses.

The first research hypothesis, positing a significant impact of cryptocurrency recognition on the assessment of RMM, was subjected to statistical analysis using the Wilcoxon Signed-Rank Test, a non-parametric statistical procedure appropriate for the comparison of two related samples. This test was employed to ascertain whether a statistically significant difference existed between the medians of the two experimental conditions. The null hypothesis (H₀) was formulated as follows: $M_1 = M_2$, where M_1 denotes the median of the sample responses under the presence of cryptocurrencies as intangible assets within the financial statements, and M_2 denotes the median of the sample responses under the absence of cryptocurrencies. The alternative hypothesis (H₁) was formulated as: $M_1 \neq M_2$, asserting a statistically significant difference between the medians of the two experimental cases as presented in Table 3.

Table 3.

Wilcoxon Signed Ranks test of H_1 (n = 130).

Variable	Cases	Min.	Max.	Mean	Median	SD	P-value (Z stat.)
Cryptocurrency recognition	Absence	0.20	0.65	0.3231	0.30	0.086	0.000 (-10.045)
	Presence	0.50	0.95	0.8385	0.90	0.080	

Using an 11-point Likert scale, ranging from 0%, representing a negligible level of associated risk, to 100%, representing a very high level of risk, participants are requested to rate the assessed RMM.

The null hypothesis (H₀) was formulated as follows: $M_1 = M_2$, where M_1 denotes the median of the sample responses under the presence of cryptocurrencies as intangible assets within the financial statements, and M_2 denotes the median of the sample responses under the absence of cryptocurrencies.

The results presented in Table 3 demonstrate a p-value of 0.000, which is substantially less than the predetermined significance level of 0.05. Consequently, the null hypothesis (H₀), which posited no statistically significant impact of cryptocurrency recognition on the assessment of RMM, was rejected. Conversely, the alternative hypothesis (H₁), asserting a statistically significant difference, was accepted. Subsequent analysis of the mean risk assessments revealed a statistically significant positive effect of cryptocurrency recognition. Specifically, the means of the sample's risk assessments in the

experimental case where cryptocurrencies were present in the financial statements (83.85% with median 90%) was substantially greater than the corresponding mean in the other case where cryptocurrencies were absent (32.31% with median 30%), thus confirming the hypothesized positive and significant effect.

Our findings are consistent with agency theory and the theory of money, as the complexities and uncertainties surrounding cryptocurrencies, including valuation challenges, regulatory ambiguity, and questions about their fundamental role as money, create opportunities and incentives for management to potentially manipulate financial reporting, thus increasing the assessed RMM. Specifically, the difficulties in establishing a reliable unit of account and store of value for cryptocurrencies, as highlighted by the theory of money, contribute to the inherent volatility and valuation challenges, providing fertile ground for managerial discretion and potential misrepresentation. This aligns with agency theory's concem about information asymmetry and the potential for managers to act in their interests rather than those of shareholders, particularly when dealing with complex and less transparent assets like cryptocurrencies. The lack of clear regulatory frameworks and accounting standards further exacerbates these concerns, making it more difficult for auditors to effectively scrutinize cryptocurrency transactions and increasing the likelihood of material misstatements going undetected.

Further, the current finding aligns with some previous studies (e.g., [17, 18, 31]) which consistently demonstrate that the recognition of cryptocurrencies in financial statements is associated with increased risk assessments by auditors. Smith and Srivastava [31] highlighted the importance of robust custody solutions to mitigate risks in the digital asset ecosystem, implying a higher risk profile for entities holding such assets. Vincent and Wilkins [18] directly addressed the challenges faced by auditors in cryptocurrency audits, emphasizing the increased inherent risk due to regulatory ambiguity and technological complexities. Harrast, et al. [17] provided empirical evidence confirming that cryptocurrency recognition significantly elevates auditors' risk assessments, further supporting the current study's findings. In essence, these studies converge on the conclusion that the presence of cryptocurrencies in financial reporting increases the perceived audit risk.

The observed findings resonate particularly strongly within the Egyptian context due to several key factors. First, they reinforce the critical importance of EAS No. 315 in guiding auditors' assessments of RMM at both the financial statement level and the assertion level, with explicit consideration of the risks of misstatement arising from fraudulent activity. Second, they highlight the inherent legal risks associated with decentralized cryptocurrencies within the Egyptian jurisdiction, given their explicit prohibition under the Central Bank and Banking Law No. 194 of 2020. This legal prohibition underscores the necessity for auditors to maintain a thorough understanding of the prevailing regulatory landscape. Finally, they underscore the Central Bank of Egypt's distinct approach to digital assets, characterized by a strategic focus on the development and potential issuance of a CBDC designed to achieve a range of policy objectives, including the enhancement of financial inclusion, the improvement of payment system efficiency, the strengthening of anti-money laundering and combating the financing of terrorism (AML/CFT) efforts, the promotion of innovation within the financial sector, the reduction of costs associated with physical currency circulation, and the alignment with evolving global trends in CBDC adoption.

Regarding the moderating role of the IT auditor expertise on the relationship between cryptocurrency recognition and their judgments about RMM, Panel A of Table 4 indicates that the mean and median of responses of auditors with low IT expertise (76.5% and 80%) were lower than those of auditors with high IT expertise (89.5% and 90%) under the presence of cryptocurrencies. To test whether these differences are significant, results of the Mann-Whitney test, as shown in Panel B of Table 4, indicated that there is a significant difference between auditors with high IT expertise and those with low IT expertise regarding their assessment of RMM whether under the presence of the cryptocurrency in the financial statements (P-value = 0.000; Z= -9.828) or its absence (P-value = 0.000; Z= -6.689) for the behalf of high experienced IT auditors. That is the median of RMM was 90% for highly experienced IT auditors under the presence of the cryptocurrency in the financial statements, and 30% under its absence. However, the median of RMM was 30% for less experienced IT auditors whether under the presence of the cryptocurrency in the financial statements. Accordingly, H₂ is accepted.

Testing of H ₂ .									
Panel A: Descriptive statistics									
IT auditor expertise	Cases		Min.	Max.	Mean	Median	SD		
High	Absence of cryp	otocurrencies	0.30	0.65	0.361	0.30	0.095		
	Presence of cryp	otocurrencies	0.80	0.95	0.895	0.90	0.034		
Low	Absence of cryp	Absence of cryptocurrencies		0.30	0.274	0.30	0.036		
Presence of cryp		otocurrencies	0.50	0.80	0.765	0.80	0.062		
Panel B. Results of Mann-Whitney test for H ₂									
		RMM assessm	nent un	der the	RMM a	ssessment	under	the	
			absence of Cryptocurrencies			presence of Cryptocurrencies			
IT auditor expertise	P-value (Z stat.)			0.000 (-9.828)					
The sample size for group A (highly experienced IT auditors) was n=73, and for group B (less experienced IT auditors)									
n=57 to test differences in the assessment of RMM between the two groups under the presence versus absence of the									

Cryptocurrencies.

Table 4.

Our finding aligns with some previous studies (e.g., [20, 21, 59]) which demonstrate a significant relationship between IT auditor expertise and the assessment of RMM. Specifically, our results corroborate the notion that variations in IT expert ise among auditors lead to discernible differences in their evaluations of these risks. This alignment suggests that similar to the findings of Maffei, et al. [59]; Parandin, et al. [21] and Lin [20] our study also finds that IT expertise influences auditors'

understanding of complex technical systems, their proficiency in using technical audit tools and techniques, their comprehension of security risks and vulnerabilities, their effectiveness in communicating with IT professionals, and their application of professional skepticism in IT-dependent environments. This convergence of findings strengthens the argument that IT expertise plays a crucial role in shaping auditors' assessments of RMM.

5.3. Robustness Checks

A sensitivity analysis was undertaken to evaluate the robustness and generalizability of the findings derived from the primary analysis of the research hypotheses. Sensitivity analysis encompasses a range of methodological approaches designed to assess the stability of research outcomes under varying conditions. These approaches include, but are not limited to, the re-examination of hypotheses across different temporal periods, the utilization of alternative measurement instruments for both dependent and independent variables, or the re-application of the research framework to a distinct population and sample. In the present study, the sensitivity analysis was operationalized through the re-testing of the research hypotheses on a distinct sample comprising academic personnel, specifically faculty members, and those pursuing graduate diplomas, Master of Business Administration, or Master's or Doctoral degrees in accounting or finance programs affiliated with the Accounting Departments of the Faculties of Commerce at Alexandria and Damanhour Universities. This indicates that the sample has the scientific background required to conduct the study.

The objective of the sensitivity analysis was to ascertain whether the findings derived from the primary analysis of the research hypotheses exhibited stability and generalizability across different study populations. To this end, the two experimental case scenarios employed in the primary analysis, one featuring financial statements explicitly excluding cryptocurrencies and the other featuring financial statements explicitly including cryptocurrencies as intangible assets, were administered to a distinct sample consisting of academic personnel, specifically faculty members, assistant professors, and teaching assistants. Data collection protocols mirrored those implemented in the primary study, encompassing direct hand delivery and retrieval of the experimental materials, coupled with opportunities for participants to engage in dialogue with the researcher and seek clarification on any ambiguities. Participants were tasked with assessing the RMM associated with intangible assets, expressed as a percentage, within both experimental case scenarios, following the methodology outlined by Saleh and Abouelela [63]. The results obtained from the sensitivity analysis demonstrated a high degree of concordance with the findings of the primary analysis, thereby providing robust support for the generalizability of the initial conclusions.

5.4. Additional Analysis

Additional analysis is defined as a methodological procedure involving the re-examination of the core relationships under study following modifications to the initial research model [63]. These modifications may entail the introduction of novel variables, which are subsequently treated as either control variables, designed to account for extraneous influences, or moderating variables, designed to assess the contingent effects of other variables on the focal relationship. The primary objective of this additional analysis is to facilitate a comparative assessment of the results obtained from the modified mod el with those derived from the original primary analysis, thereby determining the magnitude and nature of any discrepancies and evaluating the impact of these modifications on the overall conclusions drawn from the research.

Some literature (e.g., [17, 18, 63, 64]) raised a pertinent methodological question concerning whether a control variable or a moderating variable approach would be more appropriate. To address this question rigorously, the relationship posited in the second hypothesis (H₂) was re-evaluated where the moderating variable, IT auditor expertise, was retested as a control variable. This methodological shift enabled a direct comparison between the results obtained from this additional an alysis and those derived from the initial basic analysis, facilitating a comprehensive assessment of the impact of this change in variable specification. Within the specific context of the influential relationship between cryptocurrency recognition and the assessment of RMM, the additional analysis sought to ascertain whether IT auditor expertise exerted an independent influence on the assessment of RMM, distinct from and in addition to the influence exerted by cryptocurrency recognition itself.

Regression analysis additional test.						
itistics Sig.						
9.104 0.000						
0.000						
0.640						
0.637						
227.506 (0.000)						

Table 5.

IT_Exp is the IT auditor expertise as the independent variable; RMM_With_Cryp is the responses of each participant about the assessment of RMM under the presence of cryptocurrencies ranging from 0-100%. N= 130, and the level of significance is 5%.

The regression analysis was conducted to evaluate the influence of IT auditor expertise, operationalized as an independent variable, on the assessment of RMM under the recognition of cryptocurrencies, as the dependent variable. Results shown in Table 5 yielded a statistically significant result (p < 0.05, t = 15.083) with a positive coefficient (0.129), interpreting 63.7% of changes in the assessment of RMM under the recognition of cryptocurrencies. This finding provides evidence of a positive and statistically significant relationship between IT auditor expertise and the assessed level of RMM.

Importantly, this result is congruent with the findings obtained from the primary analysis, wherein IT auditor expertise was operationalized as a moderating variable. The consistency of these results across different methodological treatments of IT auditor expertise provides robust support for the conclusion that this variable plays a salient role in influencing both the relationship under investigation and the broader process of RMM assessment.

6. Conclusion

Our study investigated the influence of cryptocurrency recognition on the assessment of RMM, with a particular focus on the moderating role of IT auditor expertise in this relationship. The primary analysis provided experimental evidence of a statistically significant positive association between the presence of cryptocurrencies within financial statements and audit ors' assessments of RMM. Moreover, the findings demonstrated that IT auditor expertise exerted a statistically significant moderating effect, amplifying the positive relationship between cryptocurrency recognition and assessed risk. The robustness of these findings was subsequently corroborated through the implementation of sensitivity analysis employing an alternative sample, which reinforced the overall conclusions derived from the primary analysis.

Additionally, our study makes several contributions to the existing literature. First, it addresses the unique challenges that cryptocurrency poses to financial reporting and auditing, highlighting risks such as valuation volatility, lack of standardized accounting, security issues, and potential illicit activities. Second, it emphasizes the moderating role of IT auditor expertise, particularly in understanding complex cryptocurrency transactions, thus underlining the need for specialized skills. Specifically, the findings suggest the necessity of being an expert in IT when auditing clients dealing with cryptocurrency transactions. Third, our study addresses a salient gap in the existing literature by expanding the relatively limited body of research in Egypt. That is, the study provides experimental evidence due to the unavailability of empirical data from Egypt, a developing country, enriching the literature dominated by studies from developed economies and allowing for comparative analysis. Finally, it develops a theoretical model linking cryptocurrency, IT auditor expertise, and the assessment of RMM, contributing to a structured understanding of these relationships and setting a foundation for future research in the field.

Moreover, our findings have implications for several key stakeholders. For auditing practice, we highlight the need for enhanced IT training and expertise among auditors to effectively assess risks related to emerging technologies like cryptocurrencies. For auditing standards and regulatory bodies, we suggest the need for specific guidance on auditing entities dealing with cryptocurrencies and emphasize the importance of IT auditor competence. For accounting standard setters, this may prompt further clarification on cryptocurrency accounting. For academics, we contribute valuable insights for accounting and auditing curricula. For emerging markets, we offer relevant context for navigating the integration of cryptocurrencies. Finally, for investors and other stakeholders, we provide a better understanding of the risks associated with cryptocurrency holdings and the importance of auditor expertise in this domain.

However, our study is subject to several limitations. First, the scope of the investigation is circumscribed by its focus on the impact of cryptocurrency recognition on the assessment of RMM and the moderating influence of auditor IT expertise within the specific context of private accounting and auditing practices in the Cairo and Alexandria governorates of the Arab Republic of Egypt. Consequently, the external validity and generalizability of the findings to auditors operating in other countries remain subject to further empirical investigation. Second, the research is specifically delimited to the audit of cryptocurrencies and does not encompass other classes of digital assets, which may exhibit distinct characteristics and present unique challenges for audit risk assessment. Third, the sample employed in the experimental study is restricted to auditors employed within private accounting and auditing firms, thereby precluding direct inferences regarding the applicability of the findings to auditors working within the governmental sector. Fourth, the operationalization of IT auditor expertise as a binary variable, focusing primarily on technical knowledge, represents a simplification of a multi-faceted construct. Fifth, while methodological rigor was employed to minimize the impact of subjective biases on the risk assessment process, it is acknowledged that the inherent limitations of human judgment preclude the complete elimination of subjective influences. Sixth, our study did not directly investigate the influence of organizational culture, prior experience with cryptocurrencies, and the regulatory environment on risk assessment. Finally, it is acknowledged that the generalizability of the research findings is contingent upon the specific controls and criteria employed in defining the study population and sample and, therefore, should be interpreted with appropriate caution.

The findings of our study suggest several promising directions for future research. First, further research could investigate the influence of digital asset recognition on the efficacy of auditors' professional judgment in identifying and evaluating material weaknesses within a client's internal control framework. Second, further research could examine the potential ramifications of digital asset recognition on the reputational capital and perceived credibility of accounting and auditing firms operating within the financial reporting ecosystem. Third, a significant area for future investigation lies in the exploration of the determinants of fair value for digital assets, encompassing an examination of various valuation methodologies and their applicability across diverse economic and regulatory contexts. Fourth, future research could examine the interplay between IT expertise, organizational culture, prior experience with cryptocurrencies, and other relevant factors in shaping risk assessments related to digital assets. Finally, future research could explore the roles of other dimensions of IT expertise, such as risk management, compliance, and audit quality, in moderating the relationship between cryptocurrency recognition and RMM assessment, potentially using more nuanced measurement scales.

References

- [1] S. Rashid, O. Fayez, H. Ismail, and R. F. Khan, "Digital social support for undergraduate students during Covid-19: Pivotal support for the digital transformation," Journal of Public Health Research, vol. 10, no. 4, p. 2148, 2021. https://doi.org/10.4081/jphr.2021.2148
- M. Alenezi and M. Akour, "Digital transformation blueprint in higher education: A case study of PSU," Sustainability, vol. 15, [2] no. 10, p. 8204, 2023. https://doi.org/10.3390/su15108204
- [3] F. Alanazi and M. Alenezi, "Driving the future: Leveraging digital transformation for sustainable transportation," Journal of Infrastructure, Policy and Development, vol. 8, no. 3, p. 3085, 2024. https://doi.org/10.24294/jipd.v8i3.3085
- J.E. Marthinsen and S.R. Gordon, "Synthetic central bank digital currencies and systemic liquidity risks," International Journal [4] of Financial Studies, vol. 12, no. 1, p. 19, 2024. https://doi.org/10.3390/ijfs12010019
- Y. Liu and H. Wei, "Digital transformation and enterprise financial asset allocation," Applied Economics, pp. 1-18, 2024. [5] https://doi.org/10.1080/00036846.2024.2322578
- M. Alsadoun and F. S. Alrobai, "Influence of fintech adoption on sustainable performance via mediation role of green finance [6] and green innovation," American Journal of Business Science Philosophy, vol. 1, no. 1, pp. 61-72, 2024. https://doi.org/10.70122/ajbsp.v1i1.13
- F. Diener and M. Špaček, "Digital transformation in banking: A managerial perspective on barriers to change," Sustainability, [7] vol. 13, no. 4, p. 2032, 2021. https://doi.org/10.3390/su13042032
- N. B. Nguyen and H. D. Nguyen, "Impacts of digital transformation and basel III implementation on the credit risk level of [8] Vietnamese commercial banks," International Journal of Financial Studies, vol. 12, no. 3, p. 91, 2024. https://doi.org/10.3390/ijfs12030091
- International Auditing and Assurance Standards Board, Identifying and assessing the risks of material misstatement: [9] International standard on auditing (ISA) 315. London, U.K: IAASB, 2019.
- [10] M. Maciejasz, R. Poskart, and D. Wotzka, "Perceptions of cryptocurrencies and modern money before and after the COVID-19 pandemic in Poland and Germany," International Journal of Financial Studies, vol. 12, no. 3, p. 64, 2024. International Journal of Financial Studies, 12(3), 64. https://doi.org/10.3390/ijfs12030064
- [11] D. Goldbarsht, "Virtual currencies as a quasi-payment tool: The case of frequent-flier programs and money laundering," Journal of Money Laundering Control, vol. 25, no. 1, pp. 150-164, 2022. https://doi.org/10.1108/JMLC-11-2020-0127
- C. Z. Hern, N. Zakaria, A. Sulaiman, F. S. Min, and K. Kamaludin, "Adoption of cryptocurrencies as a means of exchange," [12] Journal of Ecohumanism, vol. 3, no. 7, pp. 3451-3467, 2024.
- [13] G. Habadi and T. Alsamara, "The legal nature of cryptocurrencies: Analyzing potential regulatory approaches in the United Arab Emirates and the Kingdom Saudi Arabia," Journal of Ecohumanism, vol. 4, no. 1, pp. 2473–2484-2473–2484, 2025.
- M. Hashemi Joo, Y. Nishikawa, and K. Dandapani, "Cryptocurrency, a successful application of blockchain technology," [14] Managerial Finance, vol. 46, no. 6, pp. 715-733, 2020. https://doi.org/10.1108/MF-09-2018-0451
- S.-F. Hsieh and G. Brennan, "Issues, risks, and challenges for auditing crypto asset transactions," International Journal of [15] Accounting Information Systems, vol. 46, p. 100569, 2022. https://doi.org/10.1016/j.accinf.2022.100569 S. Sundarasen, I. Ibrahim, A. A. Alsmady, and T. Krishna, "Corruption's crossroads: Exploring firm performance and auditors'
- [16] role in emerging markets," *Economies*, vol. 12, no. 9, p. 239, 2024. https://doi.org/10.3390/economies12090239
- S. A. Harrast, D. McGilsky, and Y. T. Sun, "Determining the inherent risks of cryptocurrency: A survey analysis," Current Issues [17] in Auditing, vol. 16, no. 2, pp. A10-A17, 2022. https://doi.org/10.2308/CIIA-2020-038
- [18] N. E. Vincent and A. M. Wilkins, "Challenges when auditing cryptocurrencies," Current Issues in Auditing, vol. 14, no. 1, pp. A46-A58, 2020. https://doi.org/10.2308/ciia-52675
- C. Feliciano and R. Quick, "Innovative information technology in auditing: Auditors' perceptions of future importance and [19] current auditor expertise," Accounting in Europe, vol. 19. no. 2, pp. 311-331, 2022. https://doi.org/10.1080/17449480.2022.2046283
- [20] C. Lin, "Are client importance and auditor expertise associated with how material misstatement corrections are disclosed?," AUDITING: A Journal of Practice & Theory, pp. 1-25, 2024. https://doi.org/10.2308/AJPT-2022-039
- K. Parandin, A. Taki, and S. M. Madineh, "Professional skepticism and auditors' assessment of the risk of material misstatement [21] with emphasis on social cognition theory," Empirical Research in Accounting, vol. 13, no. 1, pp. 161-180, 2023. https://doi.org/10.22051/jera.2023.40968.3028
- T. Eldomiaty and N. Mohab, "Cryptocurrency volatility and Egyptian stock market indexes: A note," Modern Finance, vol. 2, [22] no. 1, pp. 121-130, 2024. https://doi.org/10.61351/mf.v2i1.138
- [23] O. Abouelela, A. Diab, and S. Saleh, "The determinants of the relationship between auditor tenure and audit report lag: Evidence from an emerging market," Cogent Business & Management, vol. 12, no. 1, p. 2444553, 2025. https://doi.org/10.1080/23311975.2024.2444553
- Ministry of Investment, "Understand the entity and its environment and assess the risks of material misstatement. Egyptian [24] Auditing Standards (EAS) 315," Retrieved: https://fra.gov.eg/wp-content/uploads/2021/01/315.pdf. [Accessed 2008.
- V. D. Dragomir and V. F. Dumitru, "Recognition and measurement of crypto assets from the perspective of retail holders," [25] FinTech, vol. 2, no. 3, pp. 543-559, 2023. https://doi.org/10.3390/fintech2030031
- J. He, T. Li, B. Li, X. Lan, Z. Li, and Y. Wang, "An immune-based risk assessment method for digital virtual assets," Computers [26] & Security, vol. 102, p. 102134, 2021. https://doi.org/10.1016/j.cose.2020.102134
- A. C. Moreaux and M. P. Mitrea, "Blockchain asset lifecycle management for visual content tracking," IEEE Access, vol. 11, pp. [27] 100518-100539, 2023. https://doi.org/10.1109/ACCESS.2023.3311635
- K. Carr, "Digital assets & license protections in an age that denies class actions and mandates arbitration," Journal of Dispute [28] Resolution, vol. 2021, no. 2, pp. 335-352, 2021.
- [29] J. Wang, W. Yi, and S. Wan, "Exploration of valuation issues for digital assets," presented at the 2024 10th International Conference on Humanities and Social Science Research (ICHSSR 2024), Atlantis Press, 2024.
- [30] K. Zhu et al., "Blockchain-based digital asset circulation: A survey and future challenges," Symmetry, vol. 16, no. 10, p. 1287, 2024. https://doi.org/10.3390/sym16101287
- [31] P. Smith and N. Srivastava, A market overview of custody for digital assets. Dubai, United Arab Emirates: Deloitte Professional Services, 2020.

- [32] H. Venter, "Digital currency–A case for standard setting activity. A perspective by the Australian Accounting Standards Board (AASB)," Retrieved: https://www.aasb.gov.au/admin/file/content102/c3/AASB_ASAF_DigitalCurrency.pdf, 2016.
- [33] A. Popescu, "Blockchain innovations: More than just cryptocurrency decentralized solutions for secure transactions and data integrity," *Innovative Computer Sciences Journal*, vol. 9, no. 1, pp. 1-7, 2023.
- [34] J. Parampathu, "From securities to currencies: The regulatory consequences of adopting cryptocurrencies as legal tender," *Transnational Legal Theory*, vol. 15, no. 2, pp. 288-339, 2024. https://doi.org/10.1080/20414005.2024.2366140
- [35] D. G. Baur, K. Hong, and A. D. Lee, "Bitcoin: Medium of exchange or speculative assets?," *Journal of International Financial Markets, Institutions and Money*, vol. 54, pp. 177-189, 2018. https://doi.org/10.1016/j.intfin.2017.12.004
- [36] A. F. Aysan, M. Caporin, and O. Cepni, "Not all words are equal: Sentiment and jumps in the cryptocurrency market," *Journal of International Financial Markets, Institutions and Money,* vol. 91, p. 101920, 2024. https://doi.org/10.1016/j.intfin.2023.101920
- [37] E. Akyildirim, A. F. Aysan, O. Cepni, and Ö. Serbest, "Sentiment matters: The effect of news-media on spillovers among cryptocurrency returns," *The European Journal of Finance*, vol. 30, no. 14, pp. 1577-1613, 2024. https://doi.org/10.1080/1351847X.2024.2323454
- [38] R. Garratt and M. R. C. Van Oordt, "The crypto multiplier," Bank for International Settlements Working Papers, No. 1104, 2023.
- [39] Pricewaterhouse Coopers (PWC), "Accounting for cryptocurrency," Retrieved: https://www.pwccn.com. [Accessed 2016.
 [40] G. Thornton, "IFRS Viewpoint Accounting for crypto assets-mining and validation issues," Retrieved:
- www.grantthoronton.global.com, 2018.[41] D. Procházka, "Accounting for bitcoin and other cryptocurrencies under IFRS: A comparison and assessment of competing
- models," *The International Journal of Digital Accounting Research*, vol. 18, no. 24, pp. 161-188, 2018. https://doi.org/10.4192/1577-8517-v18_7
- [42] Deloitte, "Thinking allowed cryptocurrency: Financial reporting implications," Retrieved: http://www.deloitte.com. [Accessed 2018.
- [43] A. A. Arens, R. J. Elder, M. S. Beasley, and C. E. Hogan, *Auditing and assurance services: An integrated approach*, 16th ed. United States of America: Pearson Education, Inc, 2017.
- [44] American Institute of Certified Public Accountants, "Accounting for and auditing of digital assets," Retrieved: https://www.aicpa.org/home. [Accessed 2021.
- [45] R. Jena, "Factors influencing blockchain adoption in accounting and auditing in the face of Industry 4.0: A multi-criteria decisionmaking approach," *Journal of Accounting & Organizational Change*, 2025. https://doi.org/10.1108/JAOC-11-2023-0205
- [46] A. Masiulevičius, "Quantitatively immaterial audit misstatements matter qualitatively," *Journal of Accounting and Taxation*, vol. 16, no. 1, pp. 15-25, 2024. https://doi.org/10.5897/JAT2023.0583
- [47] P. F. Zhang and G. Shailer, "Changes in audit effort and changes in auditors' disclosures of risks of material misstatement," *The British Accounting Review*, vol. 53, no. 3, p. 100970, 2021. https://doi.org/10.1016/j.bar.2020.100970
- [48] O. Starenka, *Risk assessment in the internal control system of an enterprise*. Publishing House "Baltija Publishing". https://doi.org/10.30525/978-9934-26-307-1-9, 2023.
- [49] C. G. Calvin, "Where's the risk? Material weakness detection in advance of financial misstatement discovery," *International Journal of Auditing*, vol. 28, no. 2, pp. 251-269, 2024. https://doi.org/10.1111/ijau.12329
- [50] A. C. Bucaro and J. D. Keyser, "Classifying internal control deficiencies: The case of magnum hunter resources corporation," *Issues in Accounting Education Teaching Notes*, vol. 39, no. 2, pp. TN1-TN10, 2024. https://doi.org/10.5555/ISSUES-2022-073tn
- [51] P. M. Dechow, W. Ge, C. R. Larson, and R. G. Sloan, "Predicting material accounting misstatements," *Contemporary Accounting Research*, vol. 28, no. 1, pp. 17-82, 2011. https://doi.org/10.1111/j.1911-3846.2010.01041.x
- [52] M. Cristofaro, P. L. Giardino, S. Misra, Q. T. Pham, and H. Hiep Phan, "Behavior or culture? Investigating the use of cryptocurrencies for electronic commerce across the USA and China," *Management Research Review*, vol. 46, no. 3, pp. 340-368, 2023. https://doi.org/10.1108/MRR-06-2021-0493
- [53] D. Stoel, D. Havelka, and J. W. Merhout, "An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners," *International Journal of Accounting Information Systems*, vol. 13, no. 1, pp. 60-79, 2012. https://doi.org/10.1016/j.accinf.2011.11.001
- [54] M. Frank, E. Maksymov, M. Peecher, and A. Reffett, "Beyond risk shifting: The knowledge-transferring role of audit liability insurers," *Contemporary Accounting Research*, vol. 38, no. 3, pp. 2224-2263, 2021. https://doi.org/10.1111/1911-3846.12670
- [55] P. D. Capatan, L. H. Vong, T. H. Bui, C. F. Vinluan, A. Domingo, and M. Yuvathasan, "Crypto assets and auditing," Retrieved: https://library2.humber.ca/collections/sites/default/files/pdf/Crypto%20Assets%20and%20Auditing.pdf, 2023.
- [56] M. Coetzee, Determining the related party risks of bitcoin: A case study. South Africa: University of Johannesburg, 2023.
- [57] N. Brender, M. Gauthier, J.-H. Morin, and A. Salihi, "The potential impact of blockchain technology on audit practice," *Journal of Strategic Innovation and Sustainability Vol*, vol. 14, no. 2, p. 35, 2019. https://doi.org/10.33423/jsis.v14i2.1370
- [58] M. C. Dyball and R. Seethamraju, "The impact of client use of blockchain technology on audit risk and audit approach—An exploratory study," *International Journal of Auditing*, vol. 25, no. 2, pp. 602-615, 2021. https://doi.org/10.1111/ijau.12238
- [59] M. Maffei, R. Casciello, and F. Meucci, "Blockchain technology: uninvestigated issues emerging from an integrated view within accounting and auditing practices," *Journal of Organizational Change Management*, vol. 34, no. 2, pp. 462-476, 2021. https://doi.org/10.1108/JOCM-09-2020-0264
- [60] A. Anis, "Blockchain in accounting and auditing: Unveiling challenges and unleashing opportunities for digital transformation in Egypt," *Journal of Humanities and Applied Social Sciences*, vol. 5, no. 4, pp. 359-380, 2023. https://doi.org/10.1108/JHASS-06-2023-0072
- [61] S. A. M. Saleh, "The effect of assuring the cloud user-related cybersecurity risk management voluntary disclosure on the nonprofessional investors' judgments and decisions: The mediating role of perceived management assertions reliability-an experimental study in Egypt," *Science Journal for Commercial Research*, vol. 51, no. 4, pp. 55-112, 2023. https://doi.org/10.21608/sjsc.2023.225537.1327
- [62] M. Peytcheva, "Professional skepticism and auditor cognitive performance in a hypothesis-testing task," *Managerial Auditing Journal*, vol. 29, no. 1, pp. 27-49, 2013. https://doi.org/10.1108/MAJ-04-2013-0852

- [63] A. M. S. Saleh and M. F. M. O. Abouelela, "Determinants of the relationship between greenhouse gases emissions disclosure assurance and the quality of auditor professional judgment on materiality: an experimental study," *Journal of Accounting Research*, vol. 10, no. 4, pp. 100-158, 2023. https://doi.org/10.21608/abj.2023.321327
- [64] M. Abuaddous, H. Bataineh, and E. Alabood, "Burnout and auditor's judgment decision making: An experimental investigation into control risk assessment," *Academy of Accounting and Financial Studies Journal*, vol. 22, no. 4, pp. 1-16, 2018.